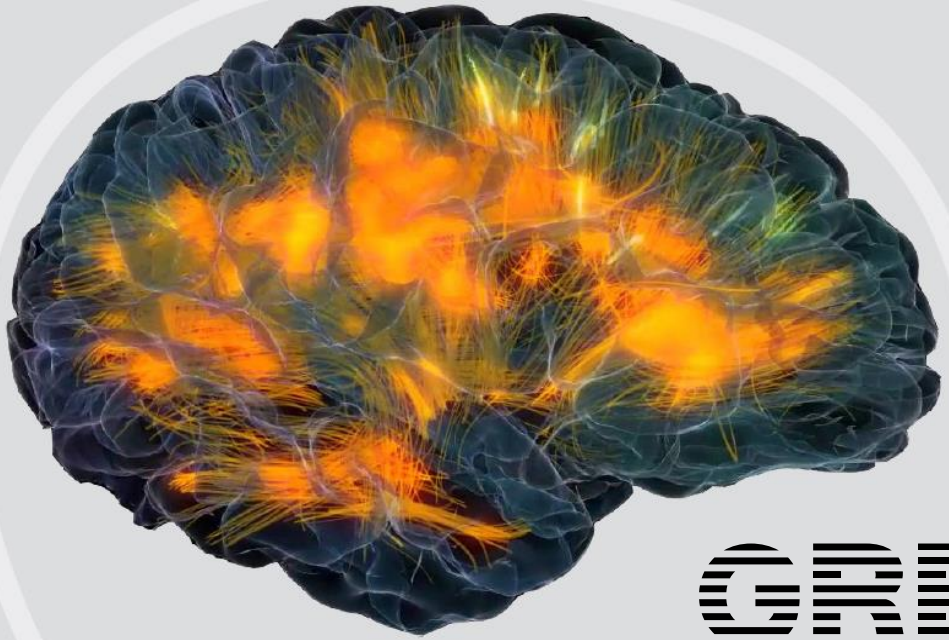


GREYCORTEX

AI ve službách bezpečnostního monitoringu sítí

CO JE GREYCORTEX?

Společnost: GREYCORTEX s.r.o., Brno
- 100% český kapitál, profesionálové v IT a veteráni kyberbezpečnosti (C|EH, CISSP, …)

Cíl: Pomáhat ochraně podniků, úřadů, kritické infrastruktury, výroby a provozu gridů
- Prostřednictvím sledování a analýzy provozu IT a OT (SCADA, ICS, Smart Buildings / Cities / Grids)

Produkt: GREYCORTEX MENDEL
- kombinace BI, ML a AI

Historie:
2009 výzkum (analýza bezp. videozáznamů - 3x cena NIST)
2013 produkt pro NTA (MENDEL)
2016 založen GREYCORTEX
2016+ spolupráce s univerzitami a dalšími (CCD COE)
2017 člen ESET Technology Alliance

Gartner Market Guide for Network Traffic Analysis 2019:
jediný dodavatel NTA v kontinentální Evropě

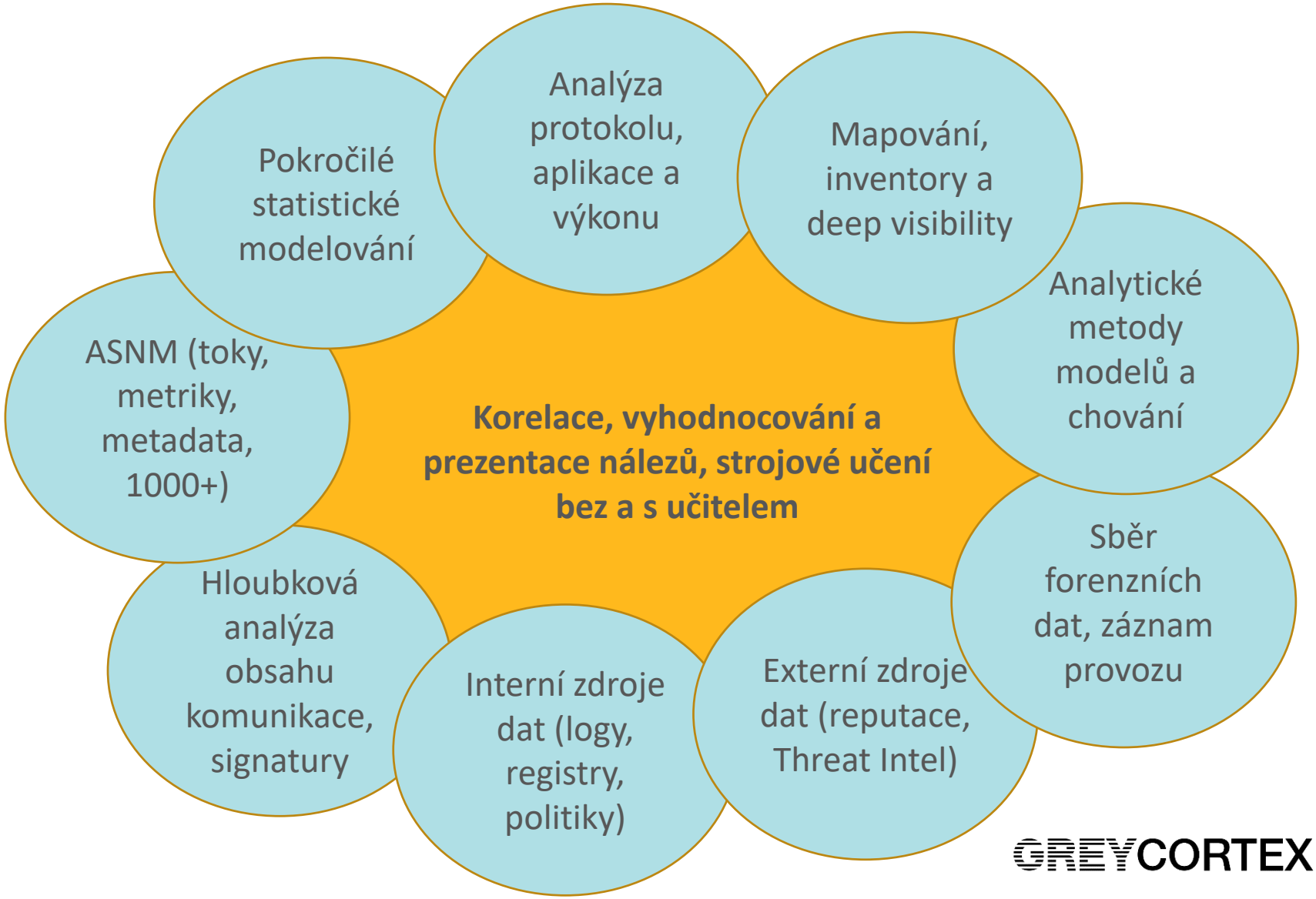
GREYCORTEX

MENDEL: Posviť na síť!

Plná síťová viditelnost a analýza dostupných dat pro síťovou bezpečnost

GREYCORTEX

ZDROJE A SOUČÁSTI ANALÝZY PROVOZU



GREYCORTEX

ZÍSKÁVÁNÍ A OBOHACOVÁNÍ DAT

Senzor: Zrcadlo provozu

- SPAN / mirror port
- TAP na lince
- Packet broker

Senzor: Automatické využití provozních informací z monitorované sítě

- DNS/DHCP
- Služby, klasifikace rolí zařízení

Konfigurace systému (při uvádění do provozu a změnách)

- Politiky, segmentace sítě a další

Kolektor: Příjem dat ze sítě

- ASNM, NETFLOW 5+, IPFIX a další
- rsyslog

Kolektor: Aktivní dotazování

- LDAP/AD
- Reputační služby

GREYCORTEX agregátor

- Signatury (Open source, komerční)
- Registry
- Aktualizace

GREYCORTEX

AUTOMATICKÁ A ASISTOVANÁ REAKCE

Integrační pluginy pro řízení firewallů a NAC

- Známí výrobci, obecné řízení
- Přizpůsobení konkrétnímu prostředí
  - Zastavení na firewallu
  - Přepojení do karantény

Zavedení a aktivace omezení provozu

- Automaticky při detekci (s následným potvrzením / zamítnutím)
- Mauálně operátorem (potvrzení nálezu)

MENDEL: Co vidíš?

Plná síťová viditelnost a analýza dostupných dat pro síťovou bezpečnost

GREYCORTEX

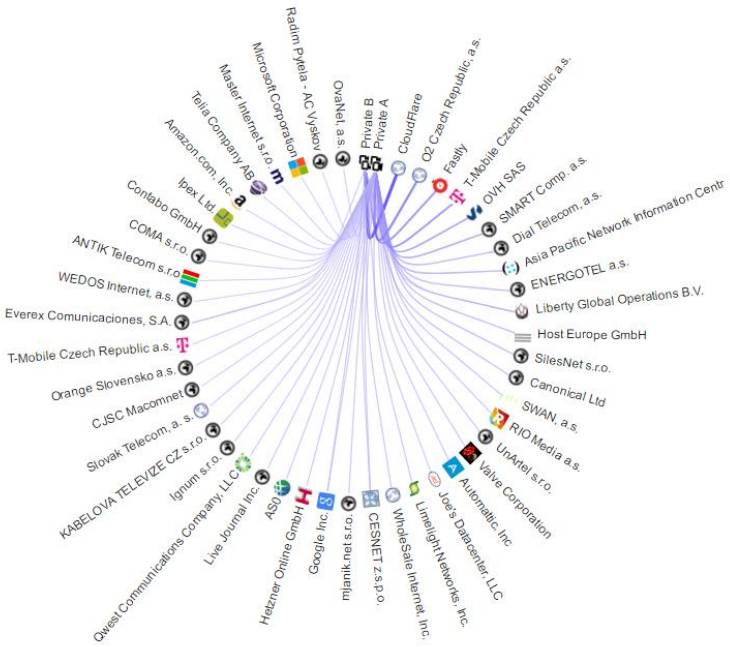
VIDITELNOST: NAJDI, ZAPIŠ A MODELUJ

Síť

- Inventory: Umístění, Addresy, ASN, Lokace
- Model: Čas, sítě, služby, metriky

Koncové zařízení

- Inventory: Umístění, Addresy,
  Služby, Protokoly
- Model: Čas, sítě, služby, protokoly, metriky
- Automatické zjištění nových zařízení
  a služeb

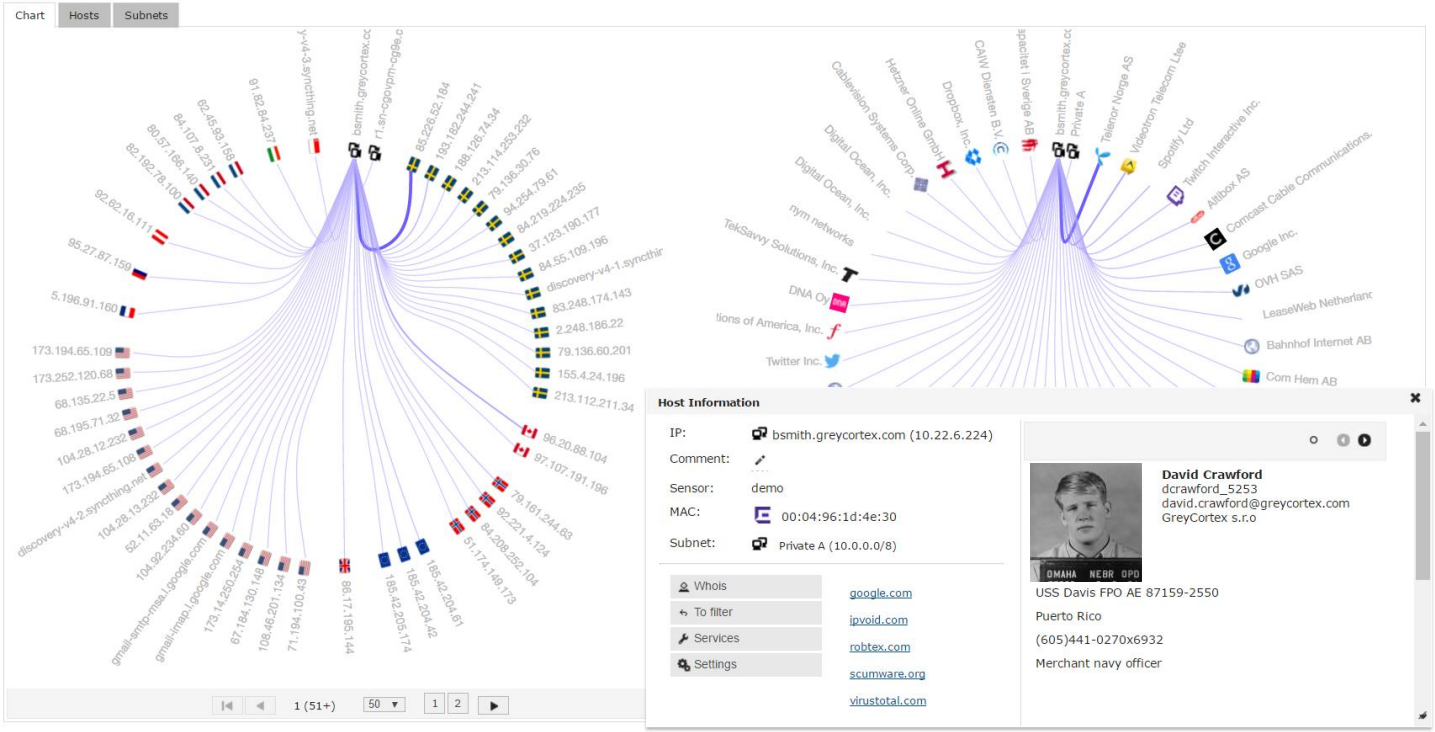


- Pouze pomocí monitoringu, analýzy a učení (nenastavuje se ručně!)

GREYCORTEX

… PŘI ANALÝZE

S kým se tenhle týpek baví?



GREYCORTEX

DETEKUJ: ANOMÁLII, HROZBU, VÝPADEK

Předpověď příští hodnoty sledovaného ukazatele

Nečekaně vysoká nebo nízká, strojově periodická

Hloubková inspekce paketů

Signaturní detekce

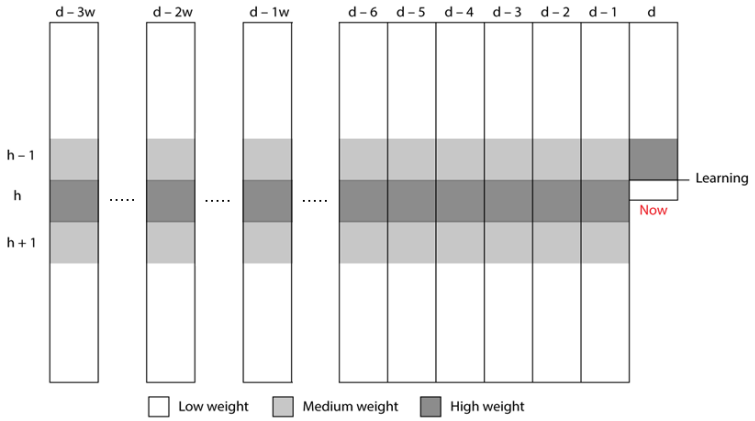
Korelace indikátorů rizik a anomálií

Profilování aplikačních dialogů

Výkon, latence, saturace

Supervizované strojové učení

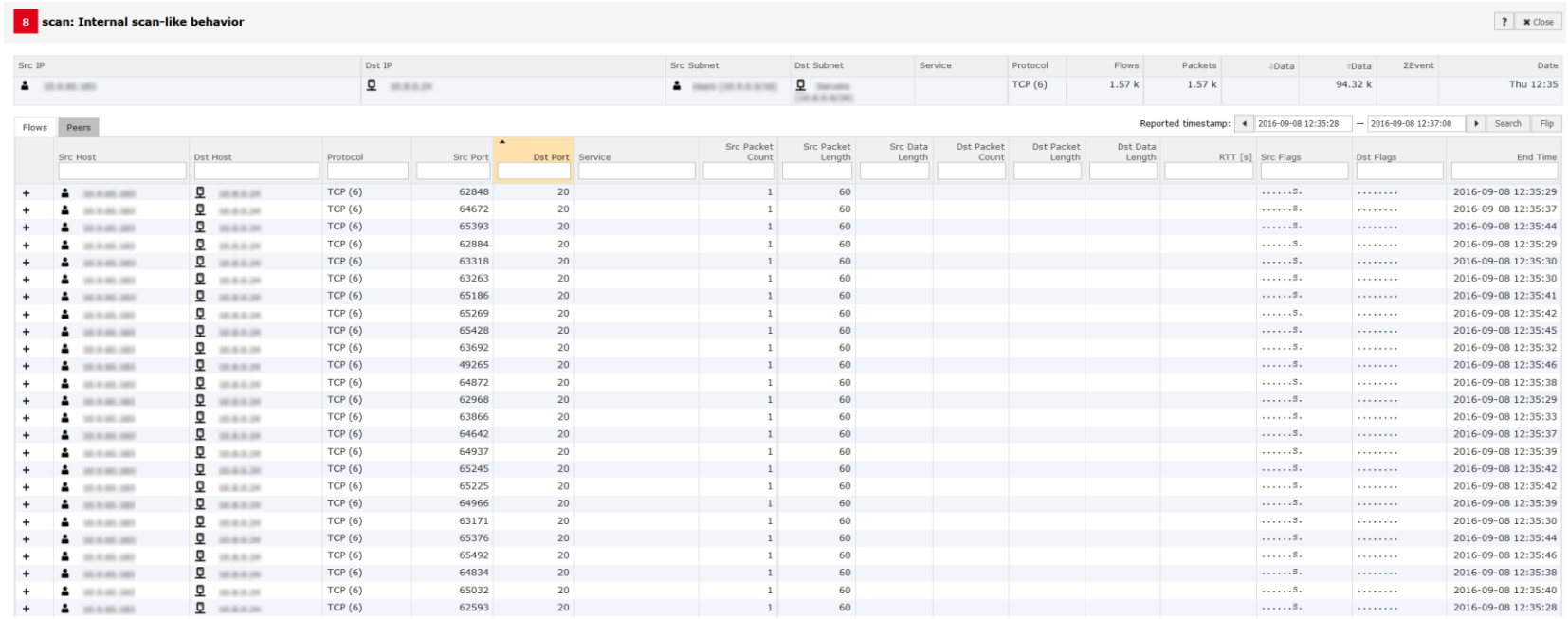
Doladění citlivosti na odchylky ukazatelů



GREYCORTEX

… PŘI ANALÝZE

Skenování portů ve vnitřní síti – rekognoskace sítě



8 scan: Internal scan-like behavior

? ✖ Close

Src IP	Dst IP	Src Subnet	Dst Subnet	Service	Protocol	Flows	Packets	↑Data	↓Data	ΣEvent	Date
[redacted]	[redacted]	[redacted]	[redacted]		TCP (6)	1.57 k	1.57 k		94.32 k		Thu 12:35

Flows | Peers

Reported timestamp: 2016-09-08 12:35:28 — 2016-09-08 12:37:00 Search Flip

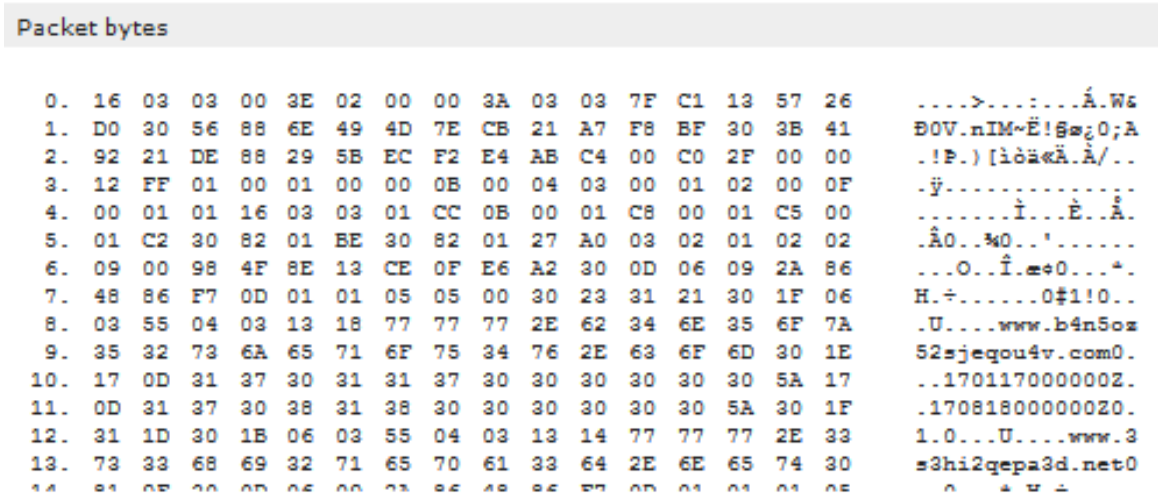
	Src Host	Dst Host	Protocol	Src Port	Dst Port	Service	Src Packet Count	Src Packet Length	Src Data Length	Dst Packet Count	Dst Packet Length	Dst Data Length	RTT [s]	Src Flags	Dst Flags	End Time
+	[redacted]	[redacted]	TCP (6)	62848	20		1	60						.....S.	.....	2016-09-08 12:35:29
+	[redacted]	[redacted]	TCP (6)	64672	20		1	60						.....S.	.....	2016-09-08 12:35:37
+	[redacted]	[redacted]	TCP (6)	65393	20		1	60						.....S.	.....	2016-09-08 12:35:44
+	[redacted]	[redacted]	TCP (6)	62884	20		1	60						.....S.	.....	2016-09-08 12:35:29
+	[redacted]	[redacted]	TCP (6)	63318	20		1	60						.....S.	.....	2016-09-08 12:35:30
+	[redacted]	[redacted]	TCP (6)	63263	20		1	60						.....S.	.....	2016-09-08 12:35:30
+	[redacted]	[redacted]	TCP (6)	65186	20		1	60						.....S.	.....	2016-09-08 12:35:41
+	[redacted]	[redacted]	TCP (6)	65269	20		1	60						.....S.	.....	2016-09-08 12:35:42
+	[redacted]	[redacted]	TCP (6)	65428	20		1	60						.....S.	.....	2016-09-08 12:35:45
+	[redacted]	[redacted]	TCP (6)	63692	20		1	60						.....S.	.....	2016-09-08 12:35:32
+	[redacted]	[redacted]	TCP (6)	49265	20		1	60						.....S.	.....	2016-09-08 12:35:46
+	[redacted]	[redacted]	TCP (6)	64872	20		1	60						.....S.	.....	2016-09-08 12:35:38
+	[redacted]	[redacted]	TCP (6)	62968	20		1	60						.....S.	.....	2016-09-08 12:35:29
+	[redacted]	[redacted]	TCP (6)	63866	20		1	60						.....S.	.....	2016-09-08 12:35:33
+	[redacted]	[redacted]	TCP (6)	64642	20		1	60						.....S.	.....	2016-09-08 12:35:37
+	[redacted]	[redacted]	TCP (6)	64937	20		1	60						.....S.	.....	2016-09-08 12:35:39
+	[redacted]	[redacted]	TCP (6)	65245	20		1	60						.....S.	.....	2016-09-08 12:35:42
+	[redacted]	[redacted]	TCP (6)	65225	20		1	60						.....S.	.....	2016-09-08 12:35:42
+	[redacted]	[redacted]	TCP (6)	64966	20		1	60						.....S.	.....	2016-09-08 12:35:39
+	[redacted]	[redacted]	TCP (6)	63171	20		1	60						.....S.	.....	2016-09-08 12:35:30
+	[redacted]	[redacted]	TCP (6)	65376	20		1	60						.....S.	.....	2016-09-08 12:35:44
+	[redacted]	[redacted]	TCP (6)	65492	20		1	60						.....S.	.....	2016-09-08 12:35:46
+	[redacted]	[redacted]	TCP (6)	64834	20		1	60						.....S.	.....	2016-09-08 12:35:38
+	[redacted]	[redacted]	TCP (6)	65032	20		1	60						.....S.	.....	2016-09-08 12:35:40
+	[redacted]	[redacted]	TCP (6)	62593	20		1	60						.....S.	.....	2016-09-08 12:35:28

GREYCORTEX

DOKUMENTUJ: ZACHYCENÝ INCIDENT

Uložené fragmenty L2-L7 vrstev a metadata

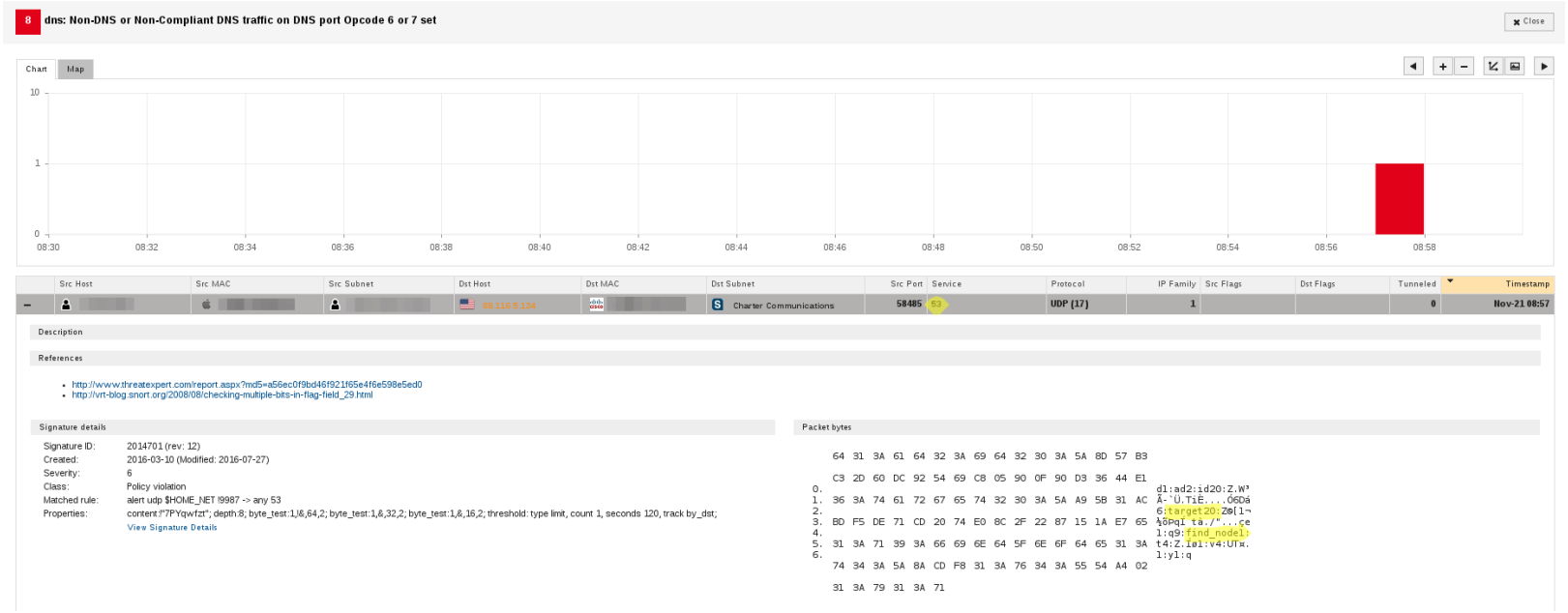
- Příznaky
- Aplikace
- Jména souborů
- Statusy odpovědí
- Hlavičky a otisk obsahu
- Tunely
- etc.



GREYCORTEX

… PŘI ANALÝZE

Komunikace přes DNS tunel na IP adresu se špatnou reputací v Číně



GREYCORTEX

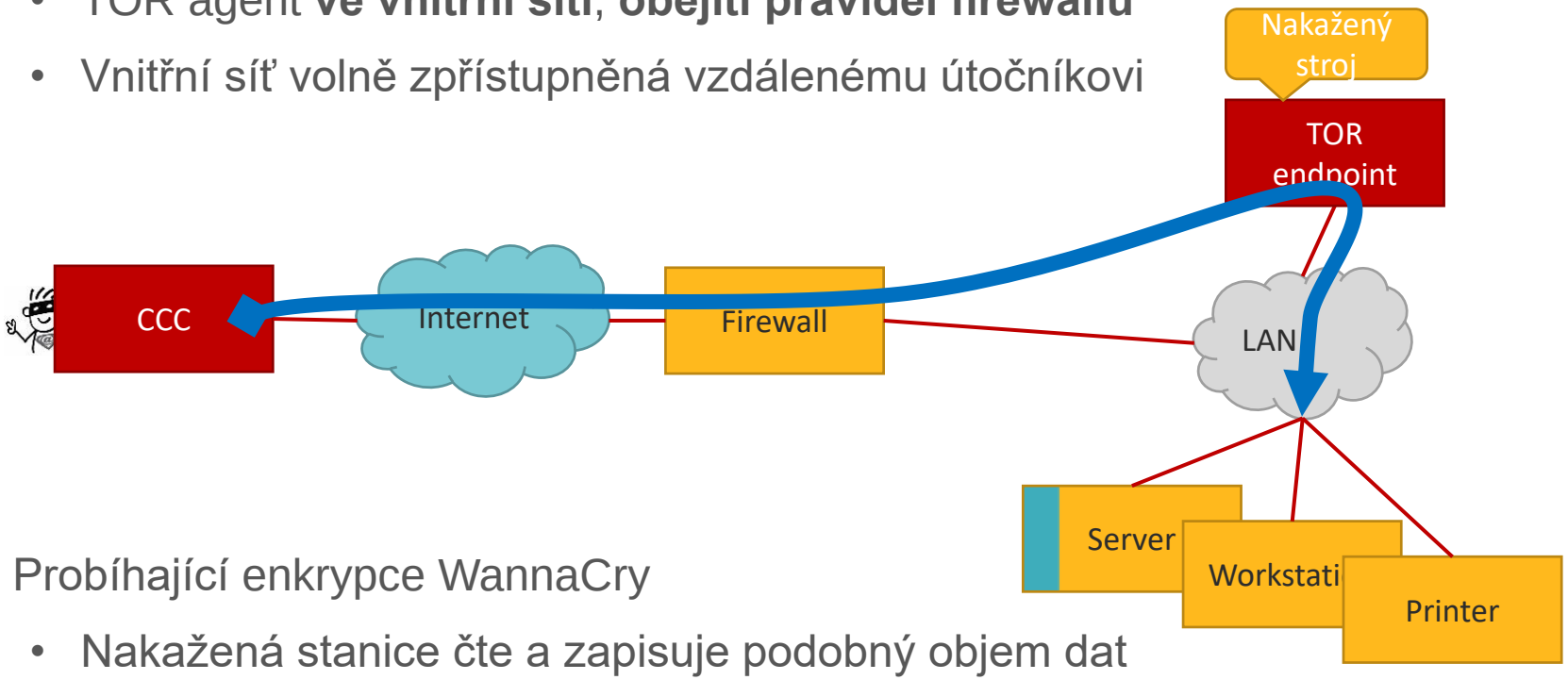
MENDEL: Co jsi našel?

Ve skutečných sítích během první hodiny od spuštění

GREYCORTEX

REZIDENTNÍ MALWARE

- VPN Filter
  - TOR agent **ve vnitřní síti**, **obejití pravidel firewallu**
  - Vnitřní síť volně zpřístupněná vzdálenému útočníkovi

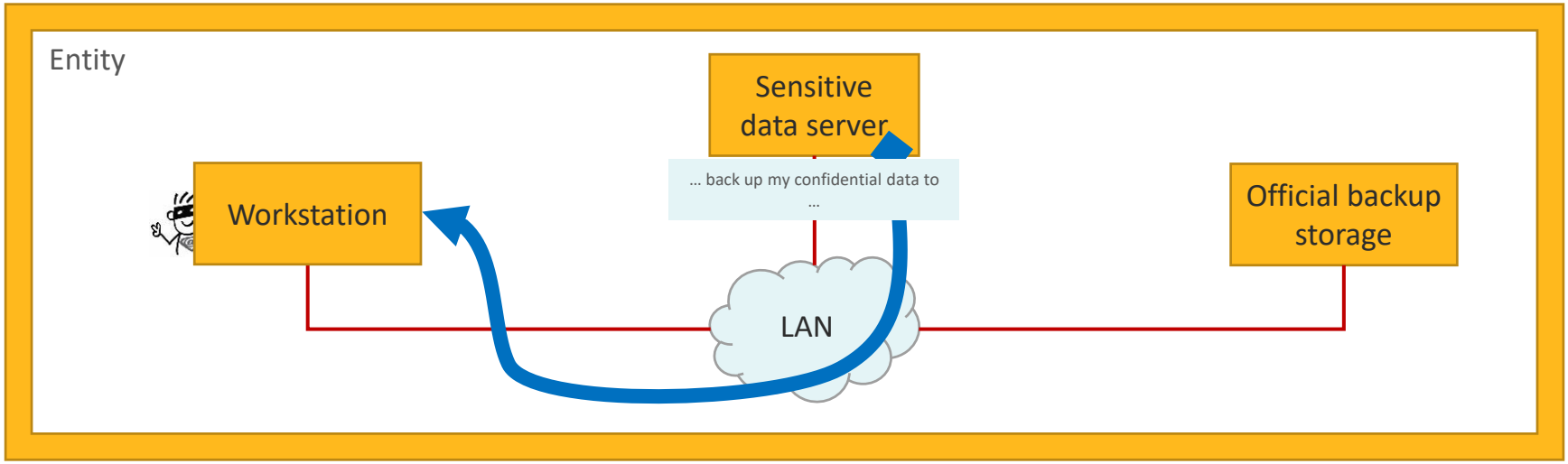


- Probíhající enkrypce WannaCry
  - Nakažená stanice čte a zapisuje podobný objem dat

GREYCORTEX

ZÁLOHOVÁNÍ CITLIVÝCH DAT NA NESPRÁVNÝ CÍL

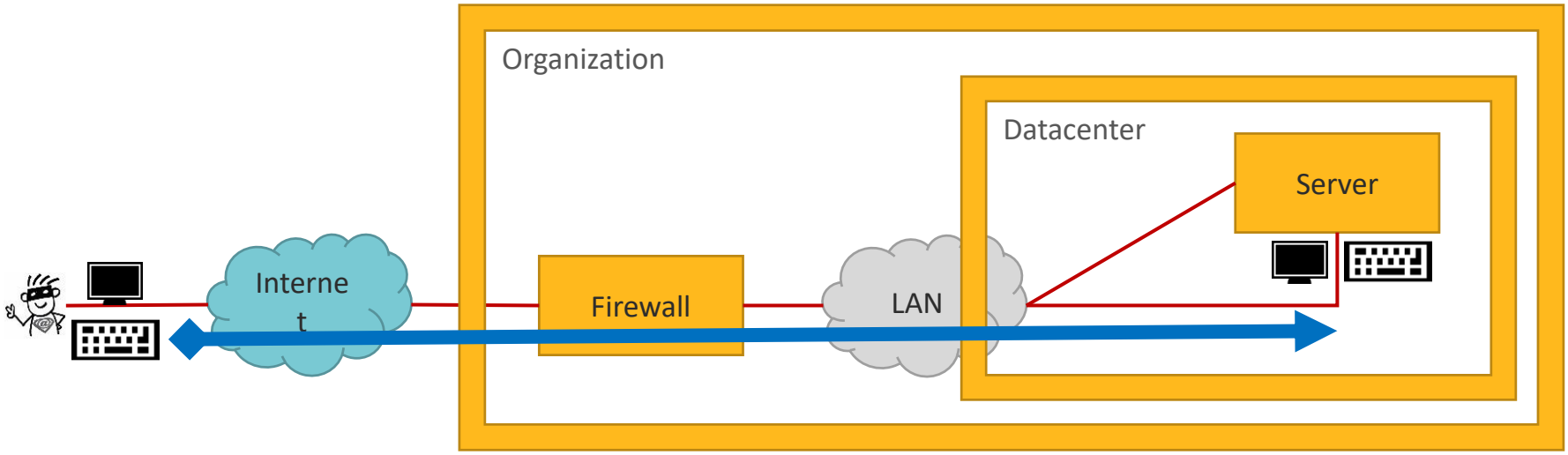
- Konfigurace zálohování použitá při testování nebyla následně opravena a citlivá data (záznamy pacientů) končila na pracovní stanici uživatele.



GREYCORTEX

VZDÁLENÁ KONZOLA SERVERU VOLNĚ PŘÍSTUPNÁ Z INTERNETU

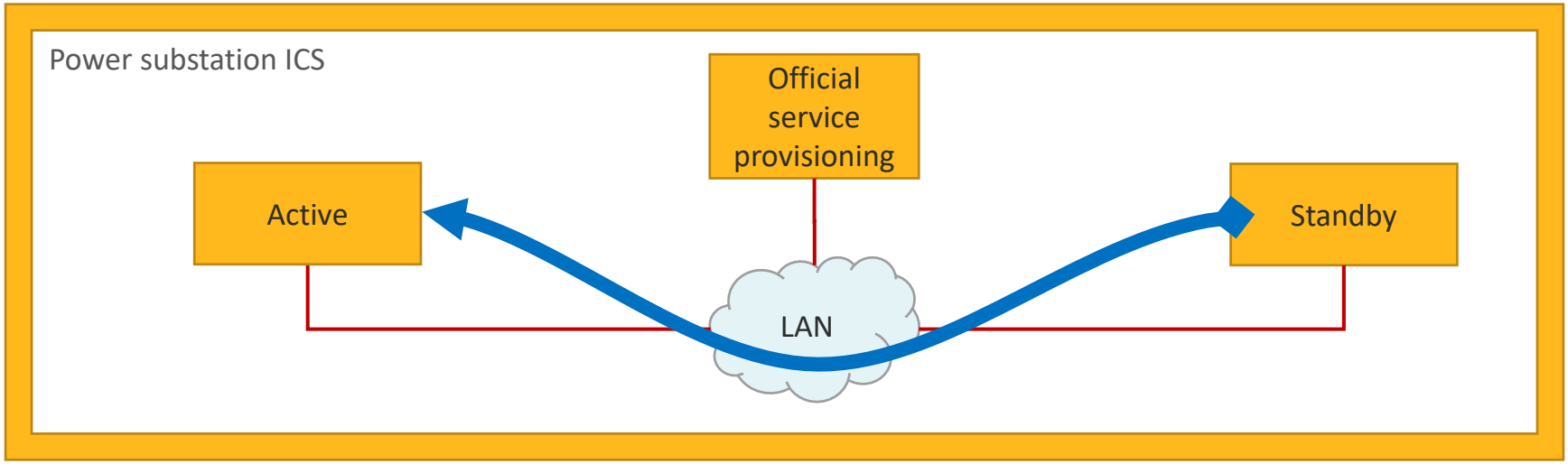
- Firewall nakonfigurovaný pro předávání portů na adresu serverového IPMI
- Vznikl tak neomezený přístup s možností instalovat software, navíc nebylo změněno výchozí heslo výrobce



GREYCORTEX

CHYBNÁ KONFIGURACE TRAFOSTANICE

- Aktivní a záložní systém si vzájemně poskytovaly služby namísto komunikace s určeným systémem. Vzniklo riziko nesprávné funkce a ohrožení dodávky energie.



GREYCORTEX

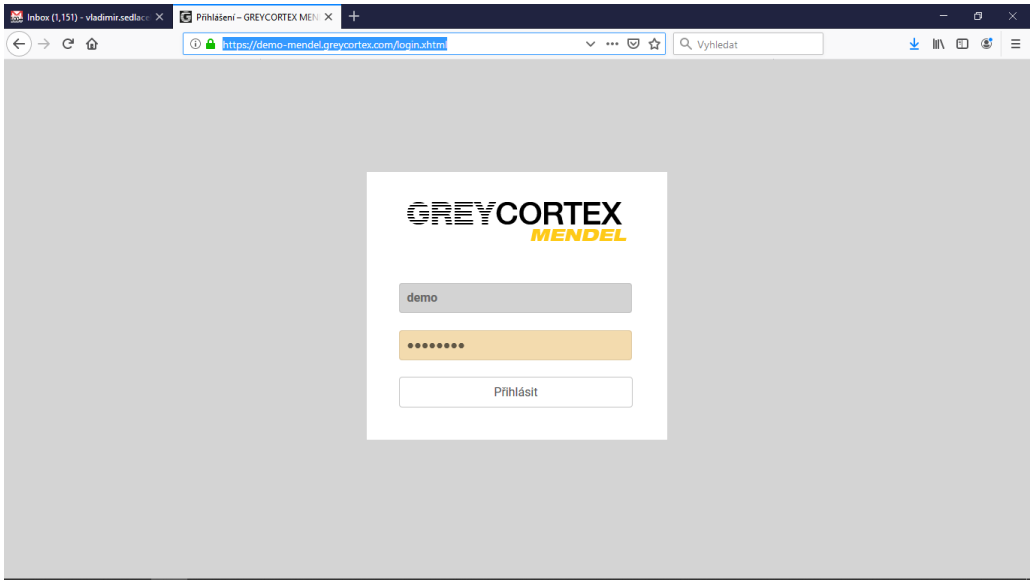
MENDEL: Tak to ukaž!

Demo, pokud se na něj dostanu…

GREYCORTEX

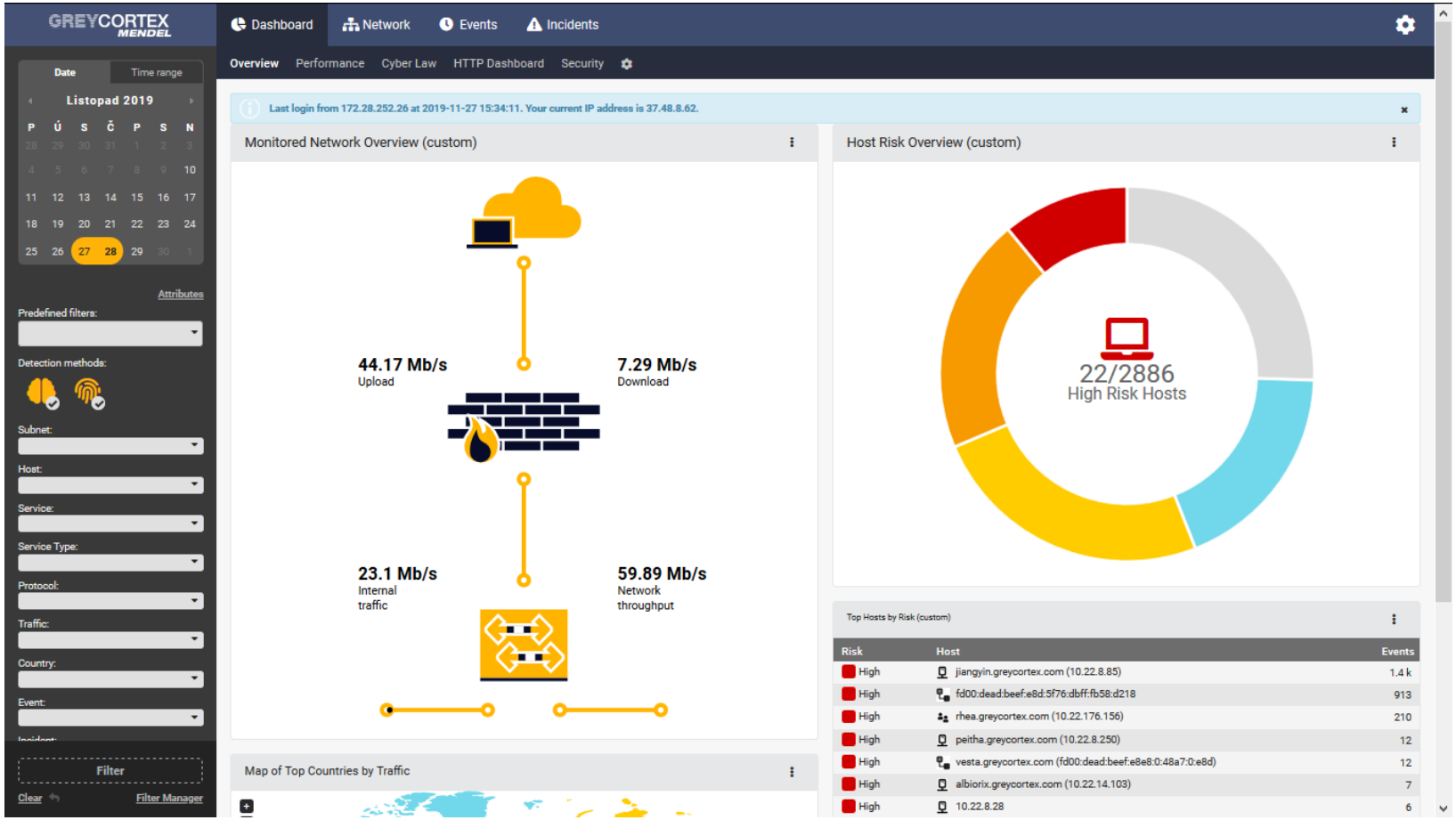
CONTINUE HERE

https://demo-mendel.greycortex.com/



GREYCORTEX

DEMO DASHBOARD



GREYCORTEX

CASE 1 – LETHIC SPAMBOT

A Device in the Observed Network:

Queried external DNS servers (Google) for known-infected server names

Communicated via port 1123 to servers in Norway

Silenced traffic when the device was running anti-virus scanner and remained silent for the next two hours, later resuming communication on port 1123

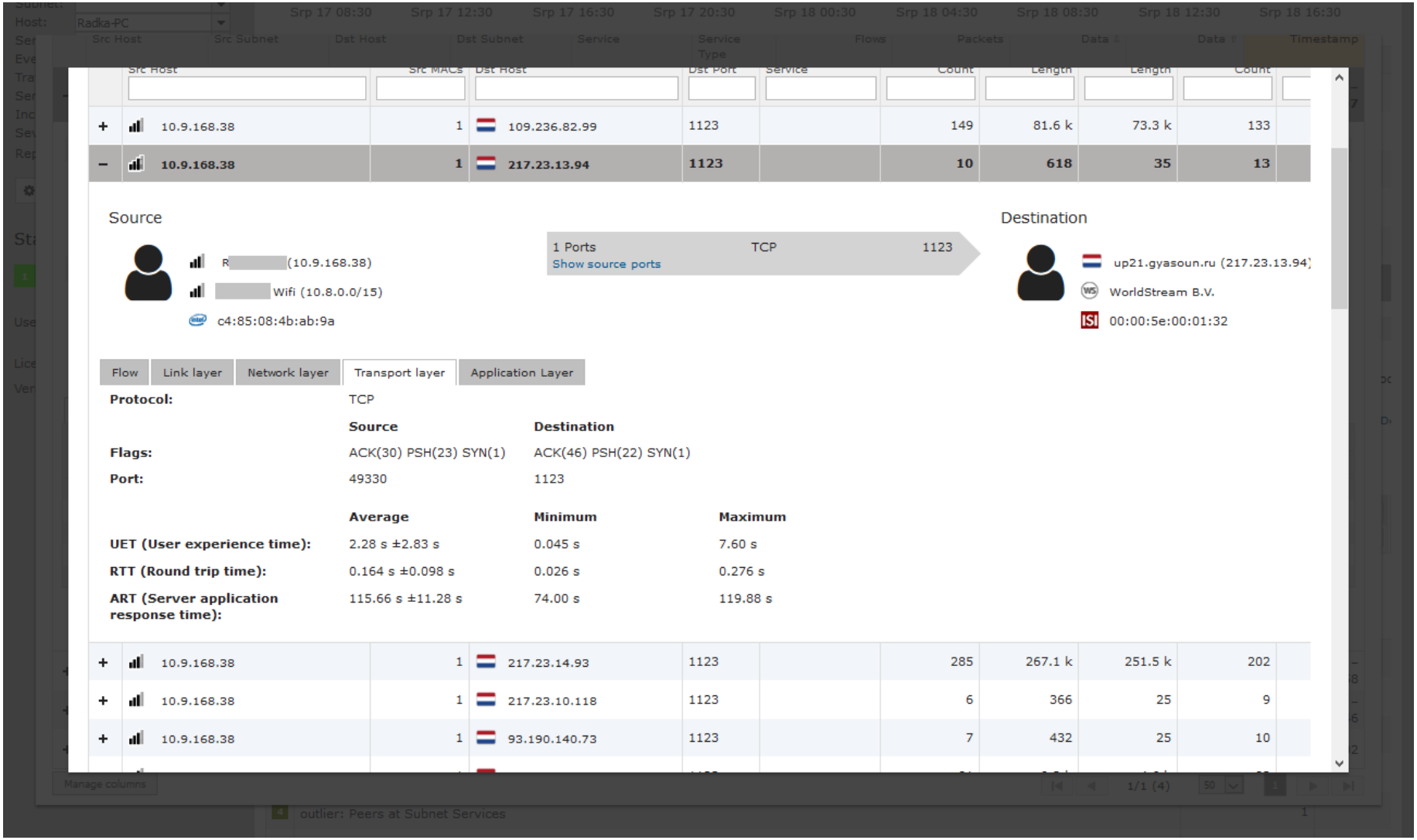
Communicated periodically to MS Hotmail service on port 25/tcp

GREYCORTEX

CASE 1 – LETHIC SPAMBOT

Unsupervised Learning	***Machine Behavior***	*Flow-based Detection*	***Discovery Analysis***	***Other***
Outlier: high number of communication peers & flows	SMTP Permanent Communication Anomaly: Communicated periodically to MS Hotmail service on port 25/tcp		A new service on a host discovered	IDS rule matched (Lethic SpamBOT) External DNS server, poor reputation Ips High external DNS traffic (1-2 queries reached170)

GREYCORTEX


Src Host
Src MACs
Dst Host
Dst Port
Service
Count
Length
Length
Count
10.9.168.38 1 109.236.82.99 1123 149 81.6 k 73.3 k 133
10.9.168.38 1 217.23.13.94 1123 10 618 35 13
Source
R (10.9.168.38)
Wifi (10.8.0.0/15)
c4:85:08:4b:ab:9a
1 Ports TCP 1123
Show source ports
Destination
up21.gyasoun.ru (217.23.13.94)
WorldStream B.V.
00:00:5e:00:01:32
Flow
Link layer
Network layer
Transport layer
Application Layer
Protocol: TCP
Source
Destination
Flags: ACK(30) PSH(23) SYN(1) ACK(46) PSH(22) SYN(1)
Port: 49330 1123
Average
Minimum
Maximum
UET (User experience time): 2.28 s ±2.83 s 0.045 s 7.60 s
RTT (Round trip time): 0.164 s ±0.098 s 0.026 s 0.276 s
ART (Server application response time): 115.66 s ±11.28 s 74.00 s 119.88 s
10.9.168.38 1 217.23.14.93 1123 285 267.1 k 251.5 k 202
10.9.168.38 1 217.23.10.118 1123 6 366 25 9
10.9.168.38 1 93.190.140.73 1123 7 432 25 10

GREYCORTEX

CASE 2 – ETERNAL BLUE

A Device on the Observed Network:

Suddenly used a DNS tunnel and TOR network together, exchanging one message

After 4 hours of waiting, it started opening port 445/tcp connections on multiple external hosts

Tried to use CVE-2017-0143 (exploit MS17-010) on the connected host

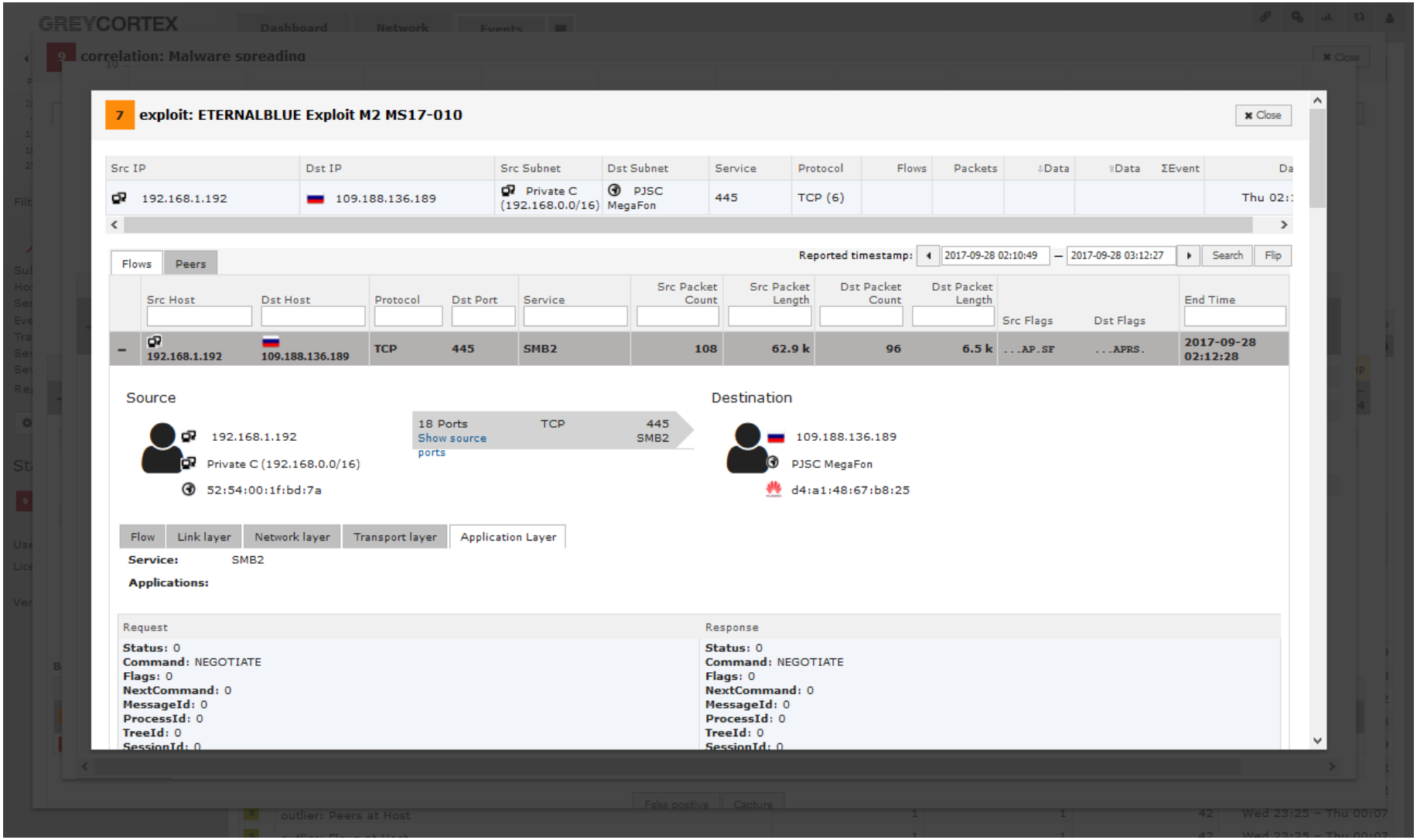
GREYCORTEX

CASE 2 – ETERNAL BLUE

Unsupervised Learning	*Machine Behavior*	***Flow-based Detection***	*Discovery Analysis*	***Other***
Outlier: high number of communication peers & flows		Network scan 445/tcp to internet		Correlation rule matched: malware spreading to internet IDS rules matched: DNS tunnel, TOR **A day after** updated IDS rule matched: Eternal Blue (based on CVE-2017-0143, exploit MS17-010)

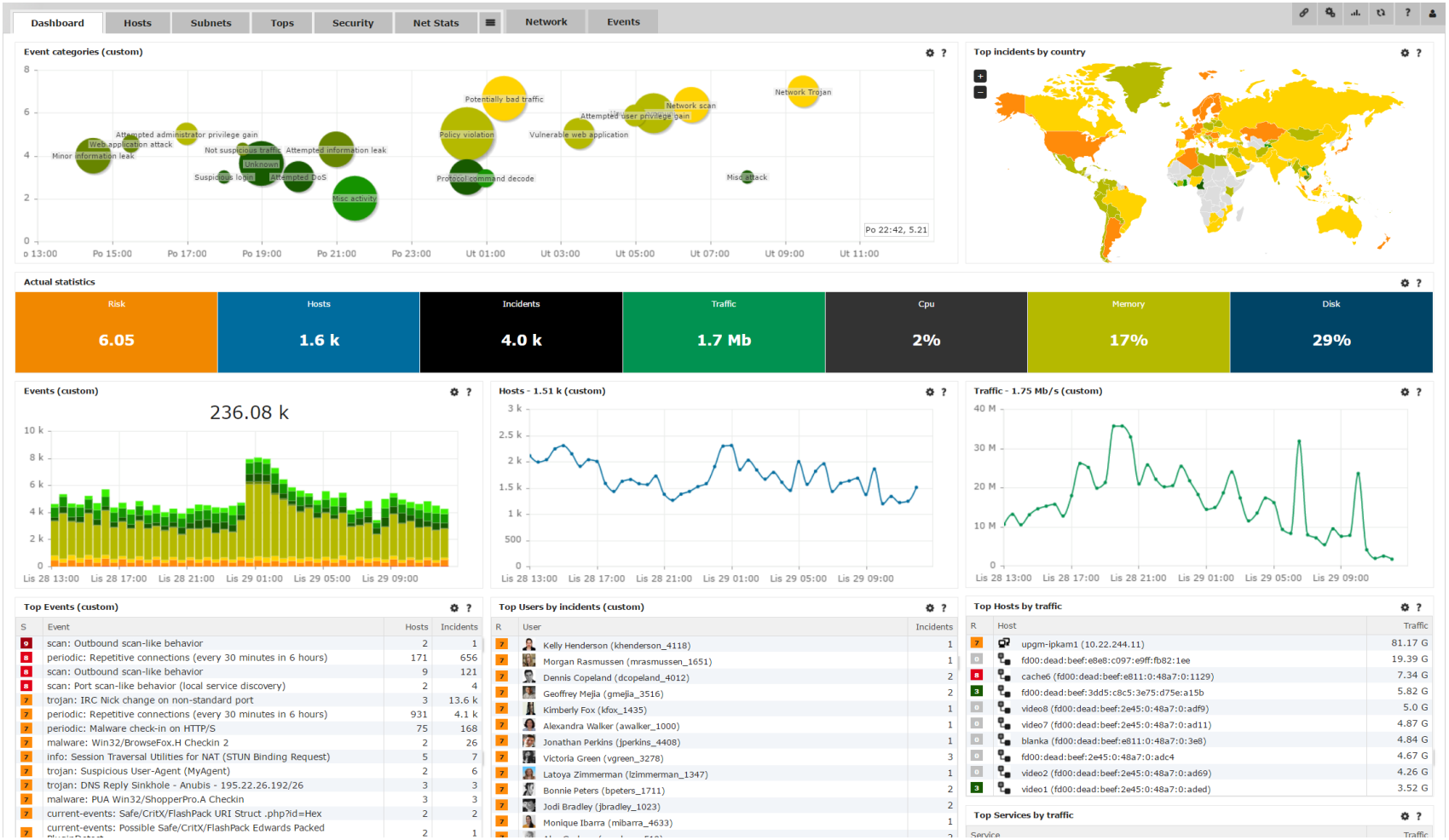
GREYCORTEX

CASE 2 - DEMO



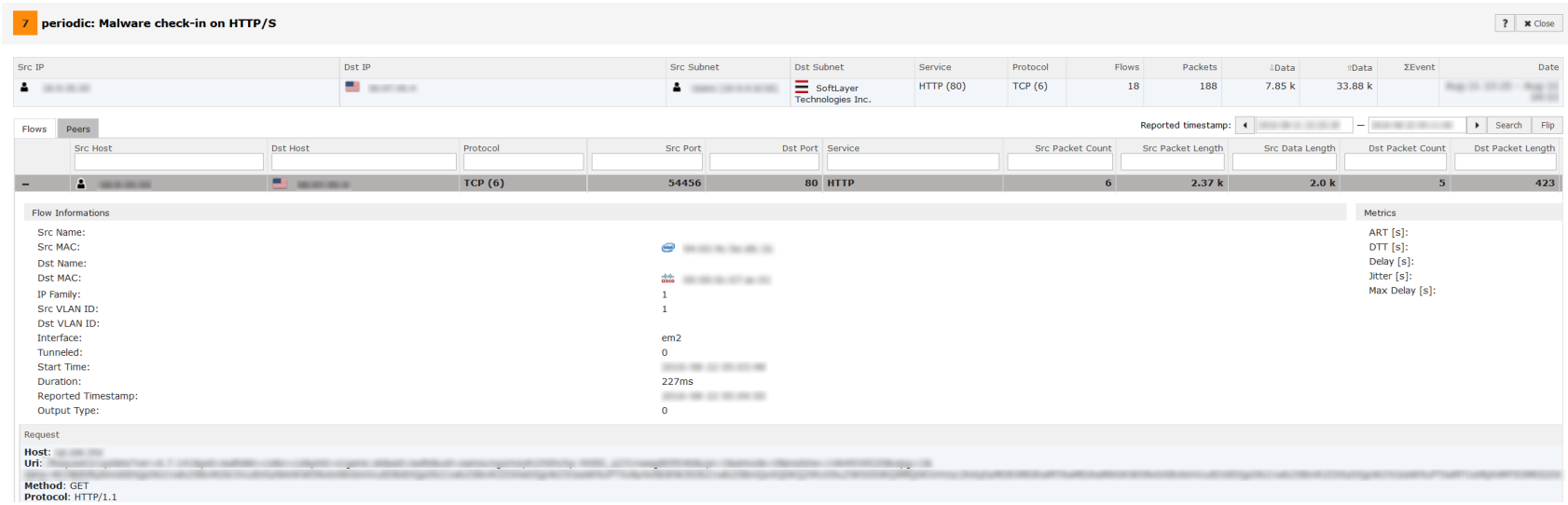
GREYCORTEX

ZÁKAZNÍKEM DEFINOVANÝ DASHBOARD



Detected Threat: Periodic Communication

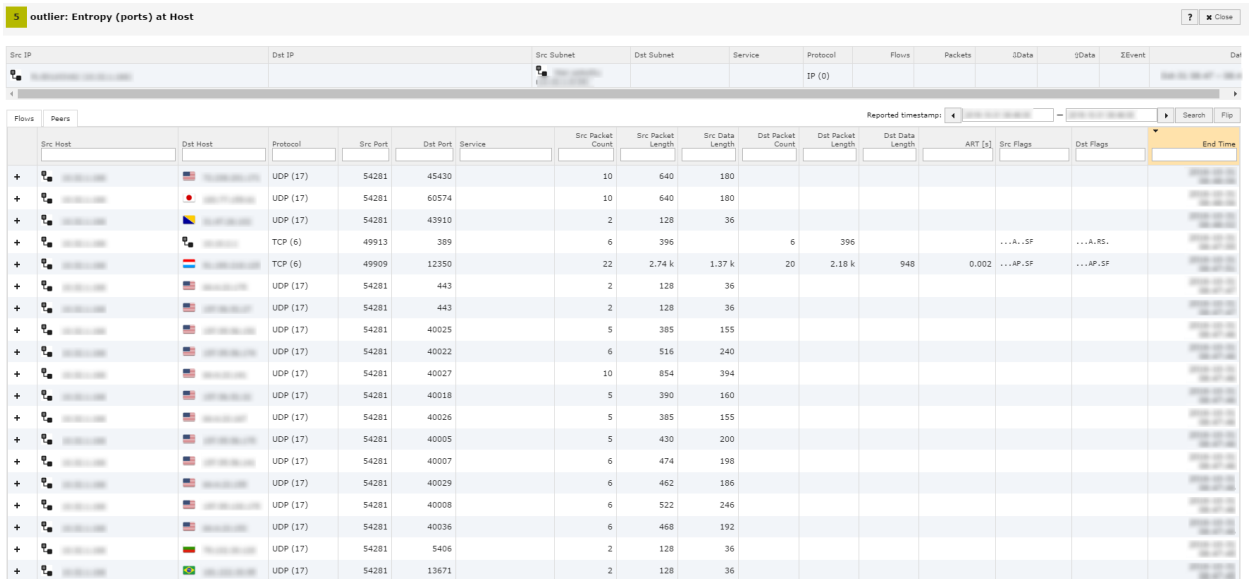
MENDEL detected periodic communication with a supposedly legitimate IP-address. The network metadata is classified as anomalous. Most likely, the user installed software with unknown malware



GREYCORTEX

Detected Threat: Excessive Communication

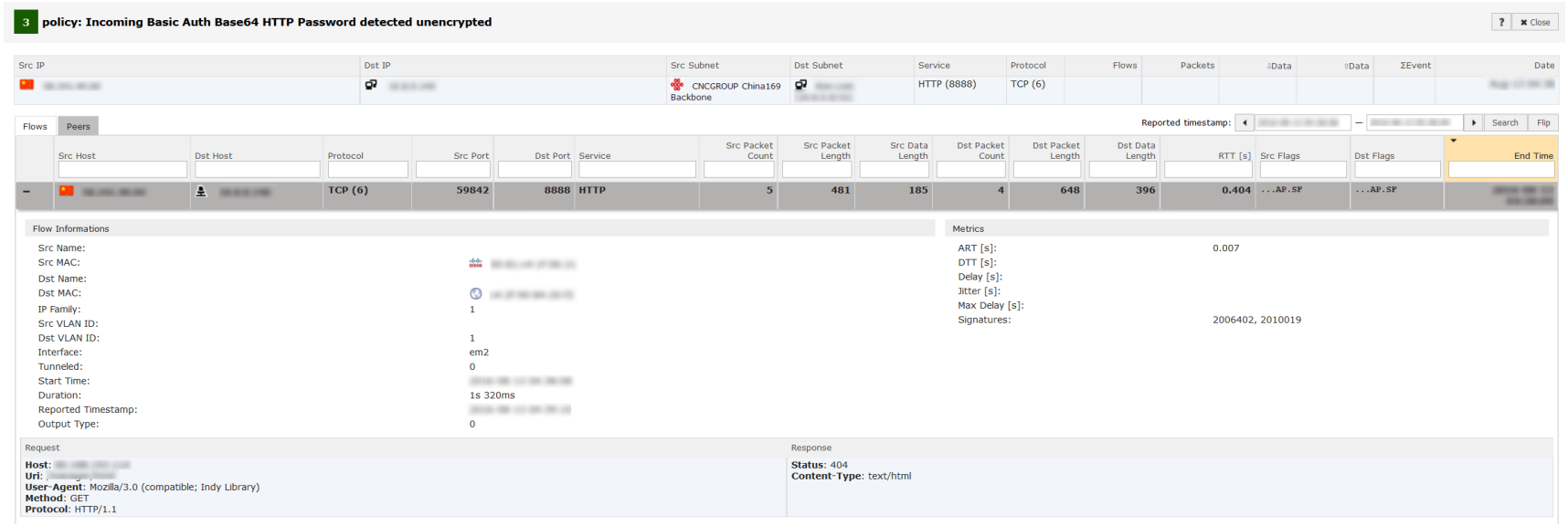
This user normally communicates through 1 to 8 network services. But, the user's device tried to communicate through 39 services, and to 120 devices around the world including Brazil, Serbia, Bosnia and Herzegovina, the United States, Singapore, and Japan. No similar communication had occurred previously in the network.



GREYCORTEX

Detected Threat: Serious Policy Breach

An exposed network device administrator with an unencrypted HTTP service resulted in an illegitimate access attempt from China. This poses a high risk for penetration and misuse.



MENDEL: Co nám dává AI!

Jak to vidí zákazníci

GREYCORTEX

AI V PRODUKTU MENDEL

Je to náš výkonný kolega, který nikdy nespí a pomáhá nám chránit se před kybernetickými útoky

Ukáže nám rychlé i pomalé útoky, skrytý provoz i vytrvalé hrozby

AI nás rychle zorientuje a vyhodnotí nám velké objemy nesouvislých dat

Soustředíme se na významné nálezy, vidíme skutečně odhalené hrozby

Takže my můžeme klidněji spát!

GREYCORTEX

Tato fotka , unknown author, 2019-06-21 18:04, CC BY-NC

Tato fotka , unknown author, 20190727-17:56, CC BY-SA

Tato fotka , unknown author, 20190727-17:56, CC BY-NC-ND

Děkuji za pozornost!

Vladimír Sedláček, CTO

vladimir.sedlacek@greycortex.com

GREYCORTEX